

Important Numbers to Report SSN, Credit Card, Check Fraud and Identity Theft

Social Security Administration
Fraud Hotline 1-800-269-0271

To order yours Social Security Earnings & Benefits Statement - 1-800-772-1213

Credit Reporting Bureaus

EquiFax To Report Fraud
800-525-6285
EquiFax Order Credit Report
800-685-1111
Experian To Report Fraud
888-397-3742
Experian Order Credit Report
800-301-7195
Trans Union To Report Fraud
800-680-7289
Trans Union Order Credit Report
800-916-8800

Fraudulent Check Use

If you've had stolen or bank accounts set up fraudulently in your name, call these check guarantee companies:

CheckRight 800-766-2748
Equifax 800-437-5120
TeleCheck 800-710-9898

They can flag your file so that counterfeit checks will be refused.

Special issues related to Identity Theft:

Occasionally, victims of identity theft are wrongfully accused of crimes committed by the imposter or attempts are made to hold them liable for civil judgments. If this occurs, contact the court where any civil judgment was entered and report that you are a victim of identity theft. If you are subjected to criminal charges as a result, quickly provide proof to the prosecutor and investigative agency.

The stress commonly experienced during identity theft victimization and recovery can be quite severe. Victims should consider seeking counseling assistance as an option, not only for yourself, but family members who may be equally traumatized.

Final Note: Your credit rating should not be permanently affected, and no legal action should be taken against you. If any merchant, financial institution or collection agency suggests otherwise, simply restate your willingness to cooperate, but don't allow yourself to be coerced into paying fraudulent bills.

Contact NCIS for additional information if you are a victim of Identity Theft.



NCIS Computer Investigations and Operations Department

Naval Criminal Investigative Service Headquarters
WNY Bldg 111 Suite 2000
716 Sicard Street SE
Washington DC 20388
WWW.NCIS.NAVY.MIL



To Protect
and Serve

NCIS United States Naval Criminal Investigative Service

Picking up the Pieces:

A Victim's Guide to Recovery from Identity Theft



NCIS Computer Investigations and Operations Department



If you are a victim of identity theft, you must document everything.

Identity theft involves someone utilizing your identifying information in order to acquire goods or services in your name through the use of credit or debit cards, checks, or other documents. In the worst cases, these identity thieves make enormous unauthorized purchases. By law, once you report the loss, theft or fraud, you have no further responsibility for



Keep a watch on your personal finances.

records requires significant effort and can take a year or even longer.

By monitoring your personal finances and following the suggestions in this brochure, you may be able to prevent or minimize losses due to issues of fraud and identity theft.

It is important to act quickly, effectively, and assertively to minimize the damage.

To prevent identity theft shred all papers containing financial and personal information before you throw them out. Also, make a list of all credit cards, ATM cards, and bank accounts and the phone numbers associated with each and keep this list in a safe place. For more actions to protect yourself, get a copy of the NCIS *Protecting Yourself from Identity Theft* brochure.

unauthorized charges. In any event, your maximum liability under federal law is \$50 per card, and most issuers will waive the fee. The bad news is that clearing up your credit

What to do: Here are the initial actions victims of identity theft should take to begin the investigative and recovery process.

1. **Report the crime to your local NCIS office and local civilian police immediately.** File a detailed police report. Give them as much documented evidence and information as possible. Keep a copy of the incident report and give it to creditors, banks, and merchants who often ask for a copy of a police report as part of the fraud investigation.

2. **Call the fraud unit at each of the big three credit bureaus to notify them of what has happened.** Request copies of your credit reports and ask the bureaus to place a "fraud alert" in your files along with a message asking future creditors to verify by telephone any applications added to your report. Follow up with a written letter.

3. **Do not pay any bill or charges that result from identity theft.** Contact all creditors immediately with whom your name has been used fraudulently - by phone and in writing.

4. **Write a "victim" statement of 100 words or less** for each of the credit bureaus to include with your credit file.

5. **Get copies of your credit reports**, following your initial report, monthly for at least several months to check for any new fraudulent accounts. The credit agency should provide these for free.

6. **Call all of your credit card issuers** to close your accounts with the notation "account closed at consumer's request" and get new credit cards with new numbers.

7. **Contact your financial institution** and request new bank account numbers, ATM cards, and checks. Put stop payments on any outstanding



Document all of your phone calls.

9. **Request a new driver's license** with an al-

ternate number from the Department of Motor Vehicles, and ask that a fraud alert is placed on your old one. Fill out a DMV complaint form to begin the fraud investigation process.

8. Give the bank, credit card and utility companies a **NEW secret password and PIN numbers** for new accounts. Do not use old PINs, passwords or your mother's maiden name.

ternate number from the Department of Motor Vehicles, and ask that a fraud alert is placed on your old one. Fill out a DMV complaint form to begin the fraud investigation process.



Get copies of, and closely inspect, your credit reports

10. **Contact the Social Security Administration** and advise them of your situation. Ask them to flag your social security number for fraudulent use. Also order a copy of your Earnings and Benefits Statement and check it for accuracy. Changing your SSN is a difficult process and should only be used as a last resort.

11. **Contact the post office and utility companies** to ensure that no billing or address changes are made to your account without a written request from you. Request that all changes be verified.

12. If you have a passport, **notify the passport office** in writing to be on the lookout for anyone ordering a new passport in your name.

13. As appropriate, **contact an attorney** to help ensure that you are not victimized again while attempting to resolve this fraud. In order to prove your innocence, be prepared to fill out affidavits of forgeries for banks, credit grantors, and recipients of stolen checks.

14. **Be persistent and follow up.** Be aware that these measures may not entirely stop new fraudulent accounts from being opened by the imposter.

NOTE: Keep detailed written records of all conversations and actions taken to recover from identity theft. Include names, titles, date/time, phone number, exact circumstances and action requested. Note time spent and any expenses incurred. Send confirmation correspondence by certified mail (return receipt).



NCIS Computer Investigations and Operations Department

Contact your local NCIS office at: